In the Claims

Please amend the claims as follows:

1. (Currently amended) An authorization device, comprising:

an integrated circuit component that in response to a first data stream, which is time-varying during at least a first time interval, generates a second encrypted data stream that **[[which]]** is time-varying and at least periodically evaluated at multiple points during **[[a]]** the first time interval to assess whether operation of a programmable logic device during the first time interval is authorized.

2. (Original) The authorization device of Claim 1, wherein the first data stream and the second encrypted data stream are time division multiplexed on an I/O pin associated with said integrated circuit component.

3. (Original) The authorization device of Claim 1, wherein said integrated circuit component utilizes an encryption operation to generate the second encrypted data stream from the first data stream.

4. (Currently amended) The authorization device of Claim 3, wherein said integrated circuit component comprises circuitry that intentionally inserts errors into the second encrypted data stream in sufficient quantity to inhibit reverse-engineering of the encryption operation .

5. (Original) The authorization device of Claim 3, wherein the encryption operation generates a first permuted bit as a function of a first bit in the first data stream and at least a first encrypted bit in the second encrypted data stream.

6. (Currently amended) ~~The authorization device of Claim 5,~~ An authorization device, comprising:

an integrated circuit component responsive to a first data stream that is time-varying during a first time interval, said integrated circuit component configured to perform an encryption operation on at least a portion of the first data stream to thereby generate a second encrypted data stream that is time-varying and at least periodically evaluated during the first time interval to assess whether operation of a programmable logic device is authorized during the first time interval;

wherein the encryption operation generates a first permuted bit as a function of a first bit in the first data stream and at least a first encrypted bit in the second encrypted data stream; and

wherein the encryption operation uses an encryption key to generate a second encrypted bit in the second encrypted data stream from at least the first permuted bit.

7. (Original) The authorization device of Claim 6, wherein the encryption operation generates a second permuted bit as a function of a second bit in the first data stream and at least the second encrypted bit in the second encrypted data stream.

8. (Original) The authorization device of Claim 7, wherein the encryption operation uses the encryption key to generate a third encrypted bit in the second encrypted data stream from the second permuted bit and the first permuted bit.

9. (Currently amended) ~~The authorization device of Claim 4,~~ An authorization device, comprising:

an integrated circuit component responsive to a first data stream that varies in time during a first time interval, said integrated circuit component configured to perform an encryption operation on at least a portion of the first data stream to thereby generate a second encrypted data stream that is time-varying and at least periodically evaluated during the first time interval to assess whether operation of a programmable logic device is authorized during the first time interval;

wherein said integrated circuit component comprises circuitry that intentionally inserts errors into the second encrypted data stream in sufficient quantity to inhibit reverse-engineering of the encryption operation; and

wherein the encryption operation generates a first permuted bit as a function of a first bit in the first data stream and at least a first encrypted bit in the second encrypted data stream.

10. (Original) The authorization device of Claim 9, wherein the encryption operation uses an encryption key to generate a second encrypted bit in the second encrypted data stream from at least the first permuted bit.

11. (Original) The authorization device of Claim 2, wherein said integrated circuit component utilizes an encryption operation to generate the second encrypted data stream from the first data stream.

12. (Original) The authorization device of Claim 11, wherein the encryption operation generates a first permuted bit as a function of a first bit in the first data stream and at least a first encrypted bit in the second encrypted data stream.

13. (Currently amended) ~~The authorization device of Claim 12,~~ An authorization device, comprising:

an integrated circuit component that in response to a first data stream generates a second encrypted data stream which is at least periodically evaluated during a first time interval to assess whether operation of a programmable logic device during the first time interval is authorized;

wherein the first data stream and the second encrypted data stream are time division multiplexed on an I/O pin associated with said integrated circuit component;

wherein said integrated circuit component utilizes an encryption operation to generate the second encrypted data stream from the first data stream;

wherein the encryption operation generates a first permuted bit as a function of a first bit in the first data stream and at least a first encrypted bit in the second encrypted data stream; and

wherein the encryption operation uses an encryption key to generate a second encrypted bit in the second encrypted data stream from at least the first permuted bit.

14. (Currently amended) The authorization device of Claim 1, wherein the first data stream is an at least weakly random sequence of bits that is generated by mixing noise and clock signals.

15. (Original) The authorization device of Claim 4, wherein the first data stream is an at least weakly random sequence of bits.

16. (Currently amended) An integrated system, comprising:

an authorization device configured to generate ~~that generates~~ a first encrypted data stream that is time-varying during a first time interval;

a programmable logic device configured to generate ~~that generates~~ a second encrypted data stream, which is time-varying during the first time interval, while simultaneously operating under at least partial control of configuration data during the **[[a]]** first time interval; and

authorization detection circuitry configured to **[[that]]** at least periodically compare ~~compares~~ the first and second encrypted data streams at multiple points during the first time interval and further configured to disable ~~disables~~ operation of said programmable logic device if the first and second encrypted data streams indicate that said programmable logic device is not authorized to utilize the configuration data during the first time interval.

17. (Original) The system of Claim 16, wherein said programmable logic device generates an at least weakly random data stream during the first time interval; and wherein said authorization device generates the first encrypted data stream in response to the at least weakly random data stream.

18. (Original) The system of Claim 16, wherein said authorization detection circuitry is internal to said programmable logic device; wherein said programmable logic device utilizes an encryption operation to generate the second encrypted data stream; and wherein each of a plurality of bits in the second encrypted data stream is determined by evaluating at least one bit in the first encrypted data stream.

19. (Original) ~~The system of Claim 17,~~ An integrated system, comprising:

an authorization device configured to generate a first encrypted data stream that is time-varying during a first time interval;

a programmable logic device configured to generate a second encrypted data stream, which is time-varying during the first time interval, while simultaneously operating under at least partial control of configuration data during the first time interval; and

authorization detection circuitry configured to at least periodically compare the first and second encrypted data streams at multiple points during the first time interval and further configured to disable operation of said programmable logic device if the first and second encrypted data streams indicate that said programmable logic device is not authorized to utilize the configuration data during the first time interval;

wherein said programmable logic device generates an at least weakly random data stream during the first time interval;

wherein said authorization device generates the first encrypted data stream in response to the at least weakly random data stream;

wherein said authorization detection circuitry operates as a dead man switch internal to said programmable logic device;

wherein said programmable logic device utilizes an encryption operation to generate the second encrypted data stream; and

wherein each of a plurality of bits in the second encrypted data stream is determined by performing the encryption operation on at least one respective bit in the first encrypted data stream and at least one respective bit in the at least weakly random data stream.

20. (Original) The system of Claim 19, wherein each of the plurality of bits in the second encrypted data stream is determined at a respective point in the first time interval by performing the encryption operation on at least one bit in the first encrypted data stream generated at an earlier point in the time interval and at least one bit in the at least weakly random data stream.

21. (Currently amended) An integrated system, comprising:

an authorization device configured to generate ~~that generates~~ a first time-varying encrypted data stream during a first time interval;

an integrated circuit device configured to generate ~~that generates~~ a second time-varying encrypted data stream and perform **[[performs]]** first operations during **[[a]]** the first time interval; and

authorization detection circuitry that at least periodically compares the first and second time-varying encrypted data streams at multiple points during the first time interval and disables operation of said integrated circuit device if the first and second time-varying encrypted data streams indicate that said integrated circuit device is not authorized to perform the first operations.

22. (Currently amended) The system of Claim 21, wherein said integrated circuit device generates an at least weakly random data stream during the first time interval; and wherein said authorization device generates the first time-varying encrypted data stream in response to the at least weakly random data stream.

23. (Currently amended) The system of Claim 21, wherein said authorization detection circuitry is internal to said integrated circuit device; wherein said integrated circuit device utilizes an encryption operation to generate the second time-varying encrypted data stream; and wherein each of a plurality of bits in the second time-varying encrypted data stream is determined by evaluating at least one bit in the first time-varying encrypted data stream.

24. (Currently amended) ~~The system of Claim 22,~~ An integrated system, comprising:

an authorization device configured to generate a first time-varying encrypted data stream during a first time interval;

an integrated circuit device configured to generate a second time-varying encrypted data stream and perform first operations during the first time interval; and

authorization detection circuitry that at least periodically compares the first and second time-varying encrypted data streams at multiple points during the first time interval and disables operation of said integrated circuit device if the first and second time-varying encrypted data streams indicate that said integrated circuit device is not authorized to perform the first operations;

wherein said integrated circuit device generates an at least weakly random data stream during the first time interval;

wherein said authorization device generates the first time-varying encrypted data stream in response to the at least weakly random data stream;

wherein said authorization detection circuitry operates as a dead man switch internal to said integrated circuit device;

wherein said integrated circuit device utilizes an encryption operation to generate the second time-varying encrypted data stream; and

wherein each of a plurality of bits in the second time-varying encrypted data stream is determined by performing the encryption operation on at least one respective bit in the first time-varying encrypted data stream and at least one respective bit in the at least weakly random data stream.

25. (Currently amended) The system of Claim 22, wherein said authorization device and said integrated circuit device are electrically connected together by a bus; and wherein the at least weakly random data stream is time division multiplexed on the bus with the first time-varying encrypted data stream.

26. (Currently amended) A method of operating a programmable logic device, comprising the steps of:

generating first and second time-varying encrypted data streams in first and second devices, respectively, during a first time interval while simultaneously operating the programmable logic device configured to perform a first operation during the **[[a]]** first time interval; and

evaluating the first and second time-varying encrypted data streams at least periodically during the first time interval and disabling operation of the programmable logic device during a subsequent second time interval if a comparison of the first and second time-varying encrypted data streams indicate that the programmable logic device is not authorized to perform the first operation during the first time interval.

27. (Currently amended) The method of Claim 26, further comprising the step of generating an at least weakly random data stream during the first time interval; and wherein the first and second time-varying encrypted data streams are generated from the at least weakly random data stream.

28. (Currently amended) The method of Claim 27, wherein the first time-varying encrypted data stream is generated internal to the programmable logic device and the second time-varying encrypted data stream is generated external to the programmable logic device.

29. (Currently amended) ~~The method of Claim 28,~~ A method of operating a programmable logic device, comprising the steps of:

generating first and second encrypted data streams in first and second devices, respectively, while simultaneously operating the programmable logic device configured to perform a first operation during a first time interval;

evaluating the first and second encrypted data streams at least periodically during the first time interval and disabling operation of the programmable logic device during a subsequent second time interval if a comparison of the first and second data streams indicate that the programmable logic device is not authorized to perform the first operation; and

generating an at least weakly random data stream during the first time interval;

wherein the first and second encrypted data streams are generated from the at least weakly random data stream;

wherein the first encrypted data stream is generated internal to the programmable logic device and the second encrypted data stream is generated external to the programmable logic device;

wherein the at least weakly random data stream is generated internal to the programmable logic device;

wherein the at least weakly random data stream is provided by a single wire bus to a device external to the programmable logic device; and

wherein the at least weakly random data stream is time division multiplexed on the bus with the second encrypted data stream.

30. (Original) The method of Claim 29, wherein the at least weakly random data stream is generated by mixing clock and noise signals.

31. (Original) The method of Claim 29, wherein each of a plurality of bits in the first encrypted data stream is evaluated by performing an encryption operation on a respective bit in the at least weakly random data stream and a respective plurality of bits in second encrypted data stream.

32. (Currently amended) An authorization device, comprising:

a first integrated circuit component that in response to a first time-varying data stream generated external to said first component generates a second time-varying data stream that is at least periodically evaluated by a distinct second integrated circuit component to assess whether performance of operations within the second integrated circuit component are authorized during a time interval when the first time-varying data stream is being generated.

33. (Currently amended) The device of Claim 32, wherein the first and second time-varying data streams are time division multiplexed on an I/O pin associated with said first integrated circuit component.

34. (Currently amended) ~~The device of Claim 32,~~ An authorization device, comprising:

a first integrated circuit component that in response to a first data stream generated external to said first component generates a second data stream that is at least periodically evaluated by a distinct second integrated circuit component to assess whether performance of operations within the second integrated circuit component are authorized during a time interval when the first data stream is being generated;

wherein the second data stream is an encrypted data stream; and

wherein each of a plurality of bits within the second data stream is generated within said first integrated circuit component using an encryption operation that is a function of at least one bit in the first data stream and at least one bit in the second data stream.

35. (Original) ~~The device of Claim 32,~~ An authorization device, comprising:

a first integrated circuit component that in response to a first data stream generated external to said first component generates a second data stream that is at least periodically evaluated by a distinct second integrated circuit component to assess whether performance of operations within the second integrated circuit component are authorized during a time interval when the first data stream is being generated;

wherein the second data stream is an encrypted data stream; and

wherein a first encrypted bit within the second data stream is generated within said first integrated circuit component using an encryption operation that is a function of at least one bit in the first data stream and a plurality of previously generated encrypted bits in the second data stream.

36. (Original) The device of Claim 35, wherein said first integrated circuit component comprises circuitry that intentionally inserts random errors into the second encrypted data stream.

37. (Currently amended) An integrated circuit system, comprising:

a first component that in response to a first time-varying data stream generated external to said first component generates a second time-varying encrypted data stream; and

a second component that at least periodically evaluates the second time-varying encrypted data stream to assess whether performance of at least one operation within the second component is authorized during a time interval when the first time-varying data stream and the second time-varying encrypted data stream are **[[is]]** being generated.

38. (Currently amended) The system of Claim 37, wherein said second component comprises an integrated circuit selected from a **[[the]]** group consisting of ASICs and PLDs.

39. (Currently amended) The system of Claim 37, wherein said second component generates the first time-varying data stream; and wherein said first and second components comprise first and second stream encryptors therein, respectively.

40. (Currently amended) The system of Claim 37, wherein said first and second components are electrically connected together by a single wire bus; and wherein the first time-varying data stream and the second time-varying encrypted data stream are time division multiplexed on the single wire bus.

41. (Currently amended) The system of Claim 39, wherein said first and second components are electrically connected together by a single wire bus; and wherein the first time-varying data stream and the second time-varying encrypted data stream are time division multiplexed on the single wire bus.

42. (Currently amended) The system of Claim 41, wherein said first component comprises circuitry that intentionally inserts random errors into the second time-varying encrypted data stream in sufficient quantity to inhibit reverse-engineering of an encryption operation used to generate the second time-varying encrypted data stream.

43. (Currently amended) ~~The system of Claim 39,~~ An integrated circuit system, comprising:

a first component that in response to a first data stream generated external to said first component generates a second encrypted data stream; and

a second component that at least periodically evaluates the second encrypted data stream to assess whether performance of at least one operation within the second component is authorized during a time interval when the first data stream is being generated;

wherein said second component generates the first data stream;

wherein said first and second components comprise first and second stream encryptors therein, respectively;

wherein the second encryptor within said second component generates a third encrypted data stream; and

wherein said second component comprises circuitry that operates as a deadman switch to disable performance of the at least one operation within said second component if the second and third encrypted data streams fail to indicate that said second component is authorized by said first component to perform the at least one operation.

44. (Currently amended) An integrated circuit system, comprising:

first and second integrated circuit devices that generate first and second time-varying data streams, respectively, while said first integrated circuit device performs software and/or hardware controlled operations during a time interval, said first integrated circuit device having authorization detection circuitry therein that receives and at least periodically evaluates the first and second time-varying data streams at multiple points during the time interval and disables the software and/or hardware controlled operations when the first and second time-varying data streams fail to indicate a sufficient match between said second integrated circuit device and the software and/or hardware controlled operations performed by said first integrated circuit device during the time interval.

45. (Currently amended) The system of Claim 44, wherein said first and second integrated circuit devices generate the first and second time-varying data streams in response to an at least weakly random sequence of bits.

46. (Currently amended) The system of Claim 45, wherein said first and second integrated circuit devices are electrically coupled together by a single wire bus; and wherein the at least weakly random sequence of bits and the second time-varying data stream are time division multiplexed on the single wire bus.

47. (Currently amended) The system of Claim 46, wherein said first integrated circuit device comprises a first stream encryptor that generates the first time-varying data stream as a first encrypted data stream from the at least weakly random sequence of bits; and wherein said second integrated circuit device comprises a second stream encryptor that generates the second time-varying data stream as a second encrypted data stream from the at least weakly random sequence of bits.

48. (Currently amended) ~~The system of Claim 47,~~ An integrated circuit system, comprising:

first and second integrated circuit devices that generate first and second encrypted data streams, respectively, while said first integrated circuit device performs software and/or hardware controlled operations, said first integrated circuit device having authorization detection circuitry therein that receives and at least periodically evaluates the first and second encrypted data streams and disables the software and/or hardware controlled operations when the first and second encrypted data streams fail to indicate a sufficient match between said second integrated circuit device and the software and/or hardware controlled operations performed by said first integrated circuit device;

wherein said first integrated circuit device comprises authorization detection circuitry that generates an error history from the first and second encrypted data streams.

49. (Original) The system of Claim 48, wherein said second integrated circuit device comprises circuitry that intentionally inserts random errors into the second encrypted data stream.

50. (Currently amended) The system of Claim 45, wherein said first integrated circuit device generates the at least weakly random sequence of bits and comprises a first stream encryptor that generates the first time-varying data stream as a first encrypted data stream from the at least weakly random sequence of bits and the second time-varying data stream; and wherein said second integrated circuit device comprises a second stream encryptor that generates the second time-varying data stream as a second encrypted data stream from the at least weakly random sequence of bits.